FIREWALL E PROXY

FIREWALL

E’ un meccanismo che consenta di controllare “il traffico in transito” e, tramite regole appositamente configurate, di inibire e/o permettere l’accesso agli indesiderati.

Nel caso di un attacco a una LAN la zona più esposta è quella intermedia e l’attaccante deve superare le difese successive del firewall che regola e limita il traffico tra i server front-end e back-end che comunicano tra loro solo su porte TCP o UDP strettamente necessarie e ben controllate.

Un firewall è un sistema hardware-software dedicato alla difesa perimetrale di una rete che agisce filtrando il traffico di pacchetti entranti e/o uscenti secondo delle regole precedentemente definite. Generalmente un firewall di rete è costituito da più macchine differenti che lavorano assieme per prevenire accessi non voluti: il router esterno, quello connesso a Internet, invia tutto il traffico entrante all’applicatione gateway che seleziona i pacchetti utilizzando apposite liste di accesso (ACL Access control list) e li inoltra alla rete interna: quindi il gateway filtra il traffico entrante e uscente, eliminando i pacchetti che non soddisfano i requisiti di sicurezza individuati (filtering router).

Nella progettazione di un firewall bisogna tenere presente tre principi fondamentali.

1. Il firewall deve essere l’unico punto di contatto della rete interna con quella esterna.
2. Solo il traffico “autorizzato” può attraversare il firewall.
3. Il firewall deve essere un sistema altamente sicuro esso stesso.

ACL Access Control List

Le regole vengono disposte in liste apposite chiamate ACL (Access Control List) dove è possibile dettagliare i filtri da applicare a ogni pacchetto in funzione delle informazioni presenti negli header TCP/IP, quindi a livello 3 (networking); a volte vengono analizzati

anche gli header di livello 4 (transport) ma si ignorano le informazioni del protocollo applicativo al quale il pacchetto si riferisce.

Le ACL si basano o su indirizzo sorgente o destinazione o sui protocolli e sui numeri di porta dei livelli superiori e le filosofie alla loro base sono due, tra loro opposte:

- open security policy: tutto è permesso per default e nella lista ACL è presente l'elenco dei divieti.
- closed security policy: tutto è vietato per default e nella lista ACL sono elencati i pochi accessi che vengono permessi, ed è la politica maggiormente adottata.

Le ACL possono anche essere inserite su qualunque router anche se trovano la loro applicazione ottimale nei router firewall posizionati tra i router interni e Internet.

Classificazione dei firewall

Una prima differenziazione viene fatta sul tipo di protezione che il firewall deve fare: come già detto, è possibile avere attacchi sia dall'esterno che dall'interno, quindi la prima classificazione riguarda proprio:

- ingress firewall : vengono controllati i collegamenti incoming, gli accessi ai servizi che sono offerti all'esterno della LAN;
- egress firewall: vengono controllati collegamenti outgoing, cioè l'attività del personale interno nella LAN verso l'esterno, in modo da filtrare il traffico in modo che quello non autorizzato o doloso non lasci mai la rete interna.

Il secondo tipo di classificazione prevede il numero di host protetti contemporaneamente:

- personal firewall: proteggono il singolo host consentendo, generalmente di default, qualsiasi traffico verso l'esterno (outbound) e bloccando quello dall'esterno (inbound);
- network firewall: si interpone fra la LAN e Internet e controlla tutto il traffico passante.

Un terzo tipo di classificazione viene fatta a seconda del livello di intervento:

- filtri di pacchetto IP: permettono di bloccare o abilitare selettivamente il traffico che attraversa il firewall, definendo i protocolli (o meglio, il tipo di pacchetto), gli indirizzi IP e le porte utilizzate;

- serventi proxy: rappresentano una sorta di intermediario che si occupa di intrattenere le connessioni per conto di qualcun altro nella rete interna.

Personal firewall

Un personal firewall può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni: in essi il traffico dall'interno verso l'esterno è consentito per default mentre il traffico dall'esterno verso l'interno è vietato per default.

I personal firewall sono utilizzabili solo a scopo personale ma impensabili in una azienda in quanto risulterebbero economicamente non convenienti e inoltre sarebbe difficile implementare una politica comune delle policy, dovendo configurare ogni singolo host manualmente.

Network firewall

Sono i classici firewall aziendali dove una (o più) macchine sono dedicate al filtraggio di tutto il traffico da e per una rete locale e solo il traffico autorizzato deve attraversare il firewall facendo in modo di mantenere i servizi di rete ritenuti necessari.

A seconda del livello di rete nel quale si fanno i controlli i network firewall possono essere classificati in:

- packet-filtering router: network level gateway.
- circuit gateway: gateway a livello di trasporto.
- proxy server: gateway a livello di applicazione.

Packet filter router

Un packet filtering router scherma i pacchetti dipendentemente dal tipo di protocollo, dall'indirizzo della sorgente e della destinazione e dai campi di controllo presenti nei pacchetti in transito, cioè analizza le informazioni contenute nell'header TCP/IP a livello di rete e di trasporto (packet inspection) per individuare:

- IP del mittente o del destinatario.
- indirizzo MAC sorgente o di destinazione.
- numero di porta verso cui è destinato il pacchetto.

- protocollo da utilizzare.

Il firewall decide se il pacchetto può essere accettato o meno attraverso un algoritmo di scelta che si basa su una lista di regole (in ordine di priorità) precedentemente definite: le filosofie applicabili come regola di funzionamento sono quindi due, diametralmente opposte:

- ciò che NON è specificatamente permesso è proibito (deny).
- ciò che NON è specificatamente proibito è permesso (permit).

e le regole di controllo possono essere configurate in modo statico (manuale) con validità temporale illimitata, oppure dinamico.

Quindi in base a queste regole i pacchetti possono essere:

- accept/allow: il firewall permette al pacchetto di raggiungere la sua destinazione.
- deny: il firewall scarta il pacchetto, senza che questo passi attraverso il firewall e viene inviato un messaggio d'errore all'host sorgente.
- discard/reject: il firewall scarta il pacchetto senza restituire nessun messaggio d'errore all'host sorgente, implementando quella che viene chiamata metodologia black hole, che elimina il pacchetto senza che la sua presenza venga rivelata agli estranei.

PROXY

Un gateway a livello di applicazione permette di realizzare una politica di sicurezza molto più severa di un semplice packet filtering router: in esso non vengono analizzati e filtrati i pacchetti ma vengono gestite le applicazioni utilizzando un apposito programma detto proxy.

Il proxy è un programma che viene eseguito sul gateway che funge da intermediario a livello di applicazione, ad esempio tra il computer dell'utente e Internet; nelle applicazioni client-server un application proxy comunica con il client simulando di essere il server, e viceversa, comunica con il server simulando di essere il client.

Mentre un packet filter è capace di utilizzare soltanto informazioni di basso livello come indirizzi IP e numero di porta, un application proxy è in grado di ispezionare l'intera porzione dati del pacchetto ed è in grado di bloccare pacchetti FTP che contengono certi nomi di file, così da inibire la connessione con determinate pagine o siti Web.

I principali **vantaggi** nell'utilizzo di un gateway a livello di applicazione sono:

- controllo completo: dato che utilizza anche le informazioni contenute nel body, effettua un doppio controllo, sia quando viene inviata la richiesta che quando si riceve la risposta.
- log dettagliati: avendo a disposizione anche le informazioni di livello applicativo produce dei file di log molto accurati.
- nessuna connessione diretta: tutti i dati in transito sono analizzati e ricostruiti: tentativi di buffer overflow o simili sono intercettati e non vengono inoltrati all'host interno.
- sicurezza anche in caso di crash: nel caso di un crash del proxy la LAN risulta isolata e quindi inaccessibile dall'esterno rimanendo protetta.
- supporto per connessioni multiple: è in grado di gestire connessioni separate che appartengono alla stessa applicazione.
- user-friendly: è semplice configurare le regole di filtraggio rispetto a quelle di un packet filtering router.
- autenticazione e filtraggio dei contenuti: offre anche il servizio autenticazione dell'utente e il
  riconoscimento dei contenuti.
- cache: effettua il caching delle pagine Web e quindi offre un ulteriore servizio liberando la rete da traffico inutile nel caso di richiesta della stessa pagina.

Per contro, gli **svantaggi** nell'uso di un gateway a livello di applicazione sono:

- è poco trasparente: richiede che ogni computer della LAN interna sia configurato per utilizzare
  il proxy.
- richiede un proxy per ogni applicazione: è necessario dedicare un proxy a ogni servizio che si
  ha necessità di far passare attraverso il firewall e, data la dinamicità con la quale vengono offerti
  servizi in rete, è necessario il suo continuo aggiornamento.
- ha basse performance: la gestione della connessione attraverso il proxy richiede molto lavoro per la CPU e quindi ha prestazioni molto inferiori rispetto ai firewall

delle generazioni recedenti.

DMZ

DMZ è la sigla di Demilitarized Zone (zona demilitarizzata) ed è una “sezione di rete” delicata e importante per i processi di sicurezza.

La zona demilitarizzata è una porzione di rete che separa la rete interna dalla rete esterna: i server nella DMZ sono accessibili dalla rete pubblica, perciò non sono trusted (dalla rete interna) e quindi devono essere segregati in quanto, se venissero compromessi, questo non deve produrre effetti collaterali nella rete aziendale.

La DMZ permette di effettuare la sicurezza perimetrale, cioè protegge una rete nei punti in cui essa
è a contatto con il mondo esterno, interponendosi tra la LAN aziendale e la WAN esterna:

- il lato LAN (local area network) è il segmento privato e protetto, e a esso appartengono tutti gli host e i server i cui servizi sono riservati all’uso interno.
- la zona WAN (wide area network) è la parte esterna, e a essa appartengono uno o più apparati di routing che sostengono il traffico da e per la rete locale, sia verso Internet che verso eventuali sedi remote dell’azienda.

La principale difesa contro gli attacchi a una rete è proprio una corretta organizzazione topologica della rete stessa; l’approccio ormai condiviso è quello di suddividere la rete in zone di sicurezza in modo che:

- i dispositivi e le risorse sono posizionati nelle zone in base ai loro livelli e requisiti di sicurezza.
- la rete acquisisce una maggiore scalabilità e una conseguente maggiore stabilità.